



のための実践情報誌

Citation 2

日経オープンシステム

NIKKEI OPEN SYSTEMS

2000
January

1



特集 ▶ p.116

21世紀の システム・エンジニアリング

製品・技術に振り回されず、変化に強いシステムを手にする

解説 ▶ p.100

不正アクセス検出ツール

ASPサービスは本当に“安い”のか?

トラブル110問(毎月)のQ&A ▶ p.220

VBで作成したC/Sアプリを

WWW環境に簡単に移行したい……ほか

今月のSecurity Check ▶ p.224

プロフェッショナル仕事を語る ▶ p.210

ランダム取締役副社長 小野 哲氏

オープンセミナー ▶ p.228

VB.NETのローカル入門

VB.NETのインターネット入門

プログラムが動く仕組み

情報システムの歴史

UNIX入門

注目技術 活用のポイント ▶ p.188

あなたはWindows 2000を導入すべきか

注目製品 選択のポイント ▶ p.198

Webアプリケーション・サーバー

Open Report

Citation 2

解説●リアルタイム監視を行う不正アクセス検出ツール

分散配置やメール監視、「仮想おとりマシン」構築機能など機能向上が進む

不正アクセスをリアルタイムに検出するツールの機能が向上している。メールやWWWアクセスの内容を監視したり、クライアントに配置して漏れなく監視する機能、「おとり」の仮想マシンを作りクラッカをおびきよせる機能を持つ製品などが出てきた。

不正アクセスをリアルタイムに検出する「IDS (Intrusion Detection System)」と呼ばれるツールの機能向上がめざましい。サーバーのログやネットワークを監視するタイプに加え、クライアントにも配置することを想定したタイプの製品が出てきた。本番稼働中のマシンの中に「おとり」となる仮想マシンを構築し、クラッカをおびきよせその行動を記録する製品も現れた(表1)。

診断からリアルタイム監視へ

不正アクセス対策ツールとしては、疑似アタックをかけてセキュリティホールや不適切なシステム設定を診断するタイプの製品の出荷数が多かったが、ここへきて「リアルタイムに検出するIDSを導入するユーザーが診断ツールと同程度に増えてきた」(ラック不正アクセス対策事業本部 ISS & Shake プロダクトチームリーダー ネットワークセキュリティ コンサルタ

ント 上原孝之氏)。診断後の監視の手段として、検出ツールの導入が広がってきている。

また、不正アクセスは社内から行われるケースも多い。監視ツールにはどのようなアクセスを検出するかをユーザーが定義できるものもある。異常なアクセス、例えば「大量データのダウンロード」や「通常行われないアクセス(例えば、システム部以外からのtelnet)」などを監視するように設定することで、社内不正アクセス対策としても使用できる。

ログなどを監視

不正アクセスを検出する方法は大きく

表1 ●日本で販売されている不正アクセス検出ツール

製品名	Cisco NetRanger	CyberCop Monitor, CyberCop Sting	HP OpenView Node Sentry	NetProwler (NP), Intruder Alert (ITA)
開発元	米Cisco Systems	米Network Associates	米Hewlett-Packard	米AXENT Technologies
日本での販売元	日本シスコシステムズ (http://www.cisco.com/jp/), ヒューコム (http://www.hucom.co.jp/) など	ネットワークアソシエイツ (http://www.nai.com/japan/)	日本ヒューレット・パカード (http://www.jp.hp.com/)	アクセント・テクノロジーズ (http://www.axent.com/), 日新電機 (http://www.einix.com/contents.html)
分類	ネットワーク監視	送受信パケット監視+ホスト監視	ネットワーク監視	ネットワーク監視 (NP), ホスト監視 (ITA)
稼働するOS	x86 Solaris	Windows NT	Windows NT (エージェント), Windows NT または HP-UX (マネージャ)	Windows NT (NP および ITA マネージャ), NT, Solaris, HP-UX, AIX, IRIX など (ITA エージェント)
価格	ハード+ソフトで247万2000円から。年間サポート45万円。価格はヒューコムによる	StingはMonitorに付属。新年度間ライセンス1ノードあたり3800円 (101ノード以上の場合は)	管理マネージャ、エージェント、それぞれ使用料100万円から	NP+ITA (1マネージャ、1エージェント) で110万円。ITAのマネージャは50万円、エージェントはUNIX版が76万円、NT Server版が24万円、NT Workstation版が2万円
販売形態	ラック・マウント型ハードウェア+ソフトウェア。管理コンソール・ソフトウェアとしてOpenView Network Node Managerが別途必要	ソフトウェア	ソフトウェア。Cisco NetRanger/ソフトウェアのWindows NT版のOEM。管理コンソールとしてOpenView Network Node Managerが別途必要	ソフトウェア

Citation 2



#1

このような攻撃パターンをシグネチャと呼ぶ。各ベンダーは100以上のアタックに対応するシグネチャを用意している。新しいセキュリティホールが発見されるとシグネチャの更新が必要になる。

[swatch]

Perlで記述されたログ監視ツール。管理者が指定したアクセスのパターンを検出するとメールなどで警告を発するように設定できる。通常シグネチャによらずログインの失敗などを監視するなどに使用する。

[DoS]

システムやサービスを停止する攻撃。SYN Flood(コネクション開始要求パケットだけを大量に送信する)、TearDrop(分解して送信したパケットのオフセット値を不正にしてパケットの再構築を不能にする)などがある。

く分けて3つある。1つは、監視対象となるマシン上で動作し、ログなどを監視するもの。ログに、アタックの時に使用されるコマンドのパターンなど特定の文字列が含まれていると不正アクセスとみなす、などの方法をとる。

UNIXを対象にしたオープン・ソース・ソフトウェアのswatch*が原理的にはこのタイプだ。欠点は、OSのパグなどを突いてシステムの機能を停止させるDoS (Denial of Service)*攻撃をほとんど防げないことだ。

純粋なホスト監視型だけを提供するベンダーは少なく、以下に述べるいずれかの方式と組み合わせている。

流れるパケットを監視

2つめは、ネットワークを監視する

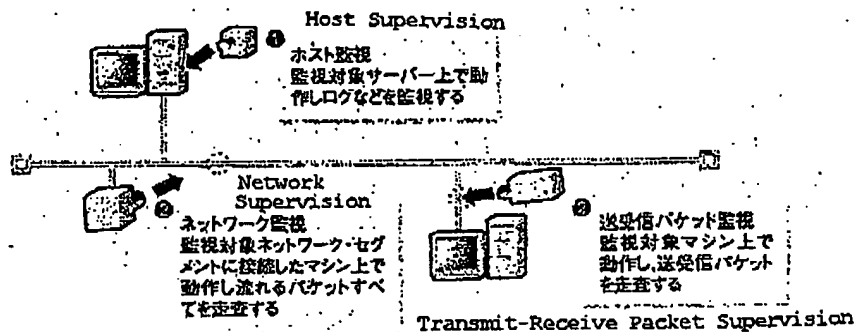


図1 ●不正アクセス監視ツールの原理

FIB. 1 Principle of Corrupt Access Supervisory Tool

もので、監視対象のネットワーク・セグメントを流れるすべてのパケットを取り込み、パケットに含まれるアタックのパターンを探す。

このようなネットワーク監視型では、監視していることをクラッカに検知されないように、IPアドレスを振

らずにネットワークにつなぐ。[ステルス・モード] などと呼ばれる。ただし、このままではほかのマシンと通信できないので、もう1枚のネットワーク・インターフェース・カードを装着し、こちらにはIPアドレスを与えて、社内など安全と思われるセグメントに

RealSecure Network Engine (RNE), RealSecure System Agent (RSA)	SecuroDetector	Session Wall-3	エンタープライズICEpac
※Internet Security Systems	※ODN Networks	※Computer Associates	※NetworkICE
アイ・エス・エス (http://www.isskk.co.jp/)	日本NCR (http://www.ncr.co.jp/), アクシオンテクノロジー (http://www.action.co.jp/)	アズジェント (http://www.asgent.co.jp/), フォーバルクリエティブ (http://www.foryal-c.co.jp/), オービックビジネスコンサルタント (http://www.obc.co.jp/)	知陽テクニカ (http://www.loyo.co.jp/)
ネットワーク監視 (RNE), ホスト監視 (RSA)	ネットワーク監視	ネットワーク監視	送信受信パケット監視, ネットワーク監視
Windows NT, Solaris など	Windows NT	Windows NT/95/98	Windows NT/95/98
RNEが1デバイス・バック107万8000円から、RSAが1デバイス・バック19万4000円から	ハードウェアで1185万円 (10セグメント監視ライセンス含む)。価格は日本NCRによる	34万4000円 (25ユーザー、初年度サポート含む) から。価格はアズジェントによる	年間ライセンス (サポート含む) 1ノードあたり7970円 (126~250ノードの場合)
ソフトウェア	ラック・マウント型ハードウェア・ファイバー・ネットワーク・スイッチ (10ポート) + ソフトウェア (※ISSのReal Secure Network Engine)	ソフトウェア	ソフトウェア。別途Microsoft SQL Serverが必要

Citation 2

*2

検出ツールが検出するマシンにはIPアドレスがないので、この場合アタックされているマシンのIPアドレスを送信元アドレスとして使いパケットを送る。

*3

同じIPアドレスで、間違ったMACアドレスを持つパケットを送って送ること、検知ツールをかく乱する手口も報告されている。MACアドレスが違えばパケットは受信側では受け取られない。一方、検知ツールはIPアドレス

で見ているため、MACアドレスの違うパケットも含めてパターンを検出する。そのため攻撃を見逃してしまう。

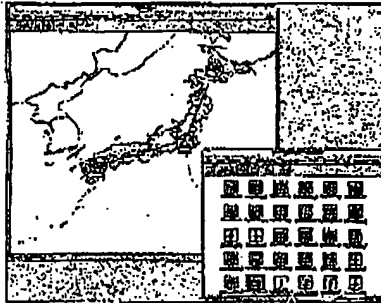


写真1 ●Cisco NetRanger
ネットワーク監視型。ハードウェアとセットで販売されている。HP OpenView上で監視、操作する。HP OpenView Node SentryはNetRangerソフトウェアのNT版のOEM製品

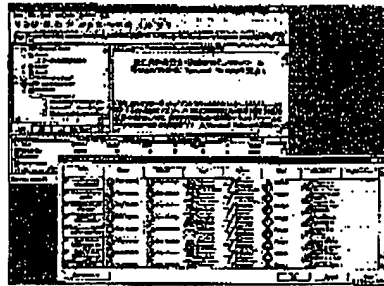


写真2 ●Session Wall-3
ネットワーク監視型で、不正アクセスのほか、ネットを流れるWWWページやメールを監視し、ルールに抵触するページやメールを保存する(背後のウインドウ)。手前のウインドウは監視ルールを定義している

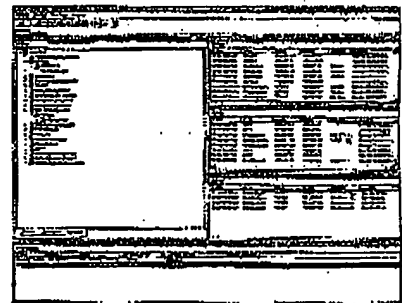


写真3 ●RealSecure Network Engine (RNE), RealSecure System Agent (RSA)
RNEはネットワーク監視型、RSAはホスト監視型で複数のマシンを集中監視する。SecureDetectorはRealSecureを組み込んだハードウェア

つなぎ、監視・設定を行う。

不正アクセスを検出すると、クラッカにリセット・パケットを送り、コネクションを強制的に切断する機能も、ほとんどの製品が備える²⁾。ファイアウォールに通知しアクセスを遮断する機能やSNMPマネージャにアラートを上げる機能を持つ製品も多い。

送受信パケットを監視

3つめは、監視対象マシンの送受信パケットを監視する方法である。ネットワーク監視型では、スイッチなどが介在すると、セグメントの全パケットは監視できない。またトラフィックが高くなると、パケットを取りこぼす可能性もある。そのため、監視対象のマシンすべてにインストールし、そのマシンあてのパケットを見る³⁾。

複数のマシンにインストールするため、監視やアップデートが1台のマシンからできるような集中管理ツールを

備えている。デメリットは検出のためのオーバーヘッドにより、性能に影響を与えることだ。オーバーヘッドが許容範囲かどうかは、マシンの性能や用途によるだろう。

OpenViewやルーターと連動

個々の製品の特徴を見ていこう。

Cisco NetRangerはネットワーク監視型のツールだ(写真1)。x86 Solarisを搭載したラック・マウント型ハードウェアに組み込まれて販売されている。Cisco製のルーターと連携することが特徴だ。不正アクセスを検出すると、ルーターに通知し、クラッカからのアクセスをフィルタリングし遮断してしまう。HP OpenView上で監視、操作するため、別途HP OpenView Network Node Managerが必要になる。

ソフトウェアのみで購入する方法もある。日本ヒューレット・パカードが販売しているHP OpenView Node

Sentryは、Windows NT版NetRangerのOEM製品である。

Session Wall-3もネットワーク監視型だが、アタック検出だけでなく、ネットワークを流れるWWW (World-Wide Web) ページやメールのパケットも監視し、検知ルールに抵触するものは保存する。この機能により、内部における不正アクセスを検知できる。

写真2の手前のウインドウは監視ルールを定義しているウインドウで、パケットの送信元やあて先、含まれる文字列などを設定し、不正と判断するアクセスおよびメール、WWWアクセスを定義する。背後のウインドウは記録したHTML (HyperText Transfer Language) を表示している。

複数方式を組み合わせる

複数の方式を組み合わせることを推奨するベンダーもある。セキュリティ・ホール診断ソフトの代表的ツール

Citation 2

オープンレポート

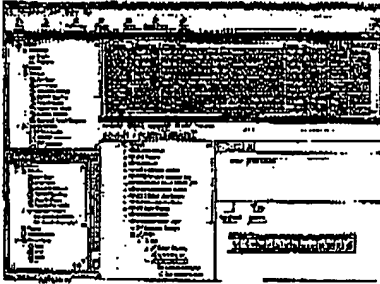


写真4 ●NetProwler (背後)とIntruder Alert (手前)
NetProwlerはネットワーク監視型で、ホスト監視型のIntruder Alertが1ライセンスが付属している

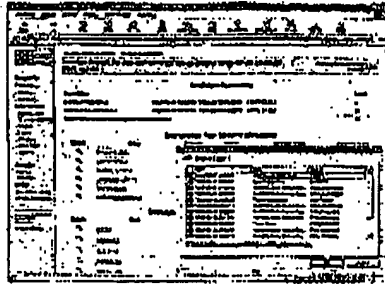


写真5 ●エンタープライズICEpac
パケット監視型とネットワーク監視型ツールからなる。クライアントに置くことを想定している。背後はレポート、手前は警告ウインドウ

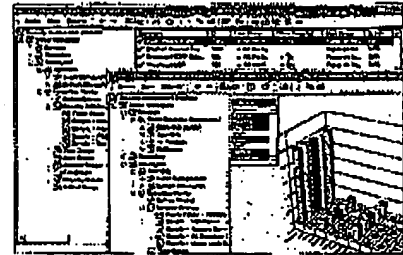


写真6 ●CyberCop Monitor
受信パケット監視とホスト監視の複合型。書き換えられたページを即座に復元する、などが可能。仮想あとリマシンを構築してクラッカをおびき寄せるCyberCop Stingが付属

Internet Scannerの開発元である米Internet Security Systemsは、ネットワーク監視型のRealSecure Network Engine (RNE)、ホスト監視型のRealSecure System Agentの2製品を販売している。1つのコンソールから両方のツールを使い、複数のマシンを集中監視できる(写真3)。検知ルールを定義する機能も備えている。

また日本NCRなどが販売するSecureDetectorは、RNEにハードウェアとスイッチを組み合わせたものだ。

ネット監視ツールにホスト監視ツールを付けて販売しているベンダーもある。NetProwlerはネットワーク監視型で、ホスト監視型であるIntruder Alertの1ライセンスが付属している(写真4)。ルール定義も可能だ。

クライアントへの配置を想定

エンタープライズICEpacはネットワーク監視型のBlackICE Sentryと、送受信パケットを監視するBlackICE

Proで構成する。BlackICE Proはクライアントにもインストールすることを想定している。分散したBlackICE Proを集中監視、アップデートするためのツールが付属している。

CyberCop Monitorはパケット監視とホスト監視の複合型で、やはりクライアントにもインストールすることを想定し、集中管理機能を持つ。

「このディレクトリは夜間書き換えられない」といった設定も可能だ。クラッカにホームページを書き換えられてもバックアップから即座に復元して被害を最小限にとどめる機能を持つ。

CyberCop Monitorに付属するCyberCop Stingは、おとりネットワークを仮想的に作る、というユニークな発想のツールだ。CyberCop Stingが動作するマシンに、本来のIPアドレスのほか複数のアドレスを割り当てておく。それぞれのIPアドレスに米Sun MicrosystemsのマシンやCiscoのルーターのふりをするように指示し

ておくと、アクセスに対しあたかもSolarisやIOS (Cisco製ルーターのOS) であるように反応する。telnetなどクラッカが狙ってくるサービスをエミュレートしており、その行動を見ていればアクセスが不正な意図を持っているかどうかわかる。

使いこなす知識は必要

残念ながら現時点では、IDSを導入しさえすれば万全という訳にはいかない。例えばアクセスの中には明らかな攻撃もあるが、グレー・ゾーンのものもある。その判断には知識が必要だ。

また、検出ルールをユーザーが設定できるタイプでは、GUIにより操作は簡単とはいえ、「手口」を知らなければ効果的な監視はできない。ベンダーのサポートなどを利用して記録を分析することが望ましい。また技術力のあるベンダーかどうかで、同じツールでも効果は変わる。

(志橋 信頼=nob@nikkeibp.co.jp)

